CLAIMS

What is claimed is:

1. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data, the decryptor being adapted to variably bit roll the encrypted data, to fixedly bit shuffle the bit-rolled data, to add a first key to the bit-shuffled data and to process the added data with a second key.

2. The system according to claim 1, wherein the decryptor is adapted to perform a single pipeline stage decryption.

3. The system according to claim 1, wherein the decryptor comprises a bit roller that rotates data in one or more roll regions of the incoming data based on an address related to the received encrypted data and a key related to the first key.

4. The system according to claim 3, wherein the key comprises a shifted version of the first key.

5. The system according to claim 3, wherein the bit roller comprises a plurality of multiplexers.

6. The system according to claim 5,

wherein each multiplexer comprises a multiplexer selection input,

wherein multiplexer selection bits are input at the multiplexer selection input, and

wherein the multiplexer selection bits are generated based on the address related to the received encrypted data and the key related to the first key.

7. The system according to claim 1, wherein the decryptor comprises a fixed bit shuffler.

8. The system according to claim 7, wherein the fixed bit shuffler comprises a fixed, hard-coded bit shuffler.

9. The system according to claim 7, wherein the fixed bit shuffler does not add a gate delay to the decryptor.

10. The system according to claim 1, wherein the decryptor comprises one or more two-bit adders.

11. The system according to claim 10, wherein each two-bit adder comprises three exclusive OR (XOR) gates and an AND gate.

12. The system according to claim 1, wherein the decryptor comprises an XOR block.

13. The system according to claim 12, wherein the XOR block comprises one or more XOR gates.

14. The system according to claim 13, wherein each XOR gate comprises a first input and a second input, the first input receiving a bit of the second key, the second input receiving a bit of the added data.

15. The system according to claim 1, wherein the first key is a shifted version of a key.

16. The system according to claim 15, wherein an amount of shift in the first key is based on an address related to the received encrypted data.

17. The system according to claim 15, wherein the first key is generated substantially in parallel with the decrypting of the encrypted data.

18. The system according to claim 1, wherein the decryptor does not add a latency to a processor pipeline.

19. The system according to claim 1, wherein the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor.

20. The system according to claim 1, wherein the decryptor decrypts a word of the encrypted data in a single cycle.

21. The system according to claim 1, wherein the word comprises a 64-bit word.

22. The system according to claim 1, wherein the decryptor is adapted to receive encrypted data from the memory.

23. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline.

24. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor.

25. A system for protecting data, comprising:

a memory in which encrypted data is stored; and

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data and decrypts a word of the encrypted data in a single cycle.

26. A system for securing data, comprising:

a processor that decrypts encrypted data, the processor being adapted to variably bit roll encrypted data and to fixedly bit shuffle the bit-rolled data.

27. The system according to claim 26, wherein the processor is adapted to perform a single pipeline stage decryption.

28. A system according to claim 26, wherein the processor is adapted to add a first key to the bit-shuffled data and to process the added data with a second key.

29. The system according to claim 26, wherein the processor is adapted to decrypt the encrypted data without adding a latency to a processor pipeline.

30. A method for securing processor instructions, comprising:

variably rolling data information based on a first key and an address related to the data information; and

hard-coded shuffling of the rolled data information;

using one or more keys to process the data information.

31. The method according to claim 30, wherein the rolling, the shuffling and the using are part of a single pipeline stage decryption.

32. The method according to claim 30, wherein using one or more keys to process the data information comprises adding the hard-coded data information and a shifted version of the first key.

33. The method according to claim 32, wherein using one or more keys to process the data information comprises processing the added data information with a second key using exclusive OR (XOR) gates.

34. The method according to claim 33, wherein the first key is unrelated to the second key.

35. The method according to claim 30, wherein the data information comprises encrypted data information.

36. The method according to claim 30,
wherein the encrypted data information is stored in a memory, and
wherein the stored data information is accessed by a processor.

37. The method according to claim 30, wherein the rolling comprises rotating bits within one or more rolling regions of the data information.